TRANG THÔNG TIN LUẬN ÁN TIẾN SĨ

Tên đề tài luận án tiến sĩ: **Xây dựng thuật toán truyền dữ liệu qua kênh thoại của mạng GSM và ứng dụng thuật toán sinh số giả ngẫu nhiên dựa trên các dãy phi tuyến lồng ghép để bảo mật dữ liệu**

Chuyên ngành:	**Kỹ thuật điện tử**
Mã số:	**9.52.02.03**
Họ và tên NCS:	**Nguyễn Thanh Bình**
Người hướng dẫn khoa học:	**GS. TSKH. Nguyễn Xuân Quỳnh**
Cơ sở đào tạo:	**Học viện Công nghệ Bưu chính Viễn thông**

NHỮNG KẾT QUẢ MỚI CỦA LUẬN ÁN:

Luận án đề cập tổng quát về mạng viễn thông di động, các lỗ hổng về bảo mật và an toàn thông tin trong mạng di động, các hình thức tấn công nghe lén, đánh cắp dữ liệu; những nghiên cứu về các phương pháp bảo mật cho mạng thông tin di động, đặc biệt là bảo mật cho truyền dữ liệu qua kênh thoại mạng GSM; nội dung nghiên cứu của luận án đã phân tích chỉ ra các khó khăn về kỹ thuật khi thực thi bảo mật cho thông tin thoại liên mạng GSM/PSTN/IP/HF/VHF để đáp ứng với yêu cầu thực tế ứng dụng cho lực lượng quốc phòng, an ninh, từ đó Luận án đã luận giải các vấn đề cốt lõi cần giải quyết về Vocoder, điều chế thành tín hiệu giả thoại, xây dựng thuật toán mã hóa. Kết quả là Luận án đã đề xuất phương pháp và xây dựng mô hình, giải pháp kỹ thuật mã thoại, điều chế dữ liệu tựa ngẫu nhiên (*dữ liệu thoại sau nén đã được sử dụng dãy phi tuyến lồng ghép 2 chiều mã hóa*) thành dạng tín hiệu tương tự có cấu trúc phổ tần gần giống với phổ tần của tiếng nói để tránh được các bộ phân tích và nhận dạng tiếng nói trên các thiết bị đầu cuối và trên các thiết bị trong hệ thống mạng viễn thông và có khả năng xuyên qua các mạng truyền dẫn trên và đáp ứng yêu cầu bảo mật mức cao nhất, thiết kế cấu hình phần cứng cụ thể thực thi giải pháp và các thuật toán để ứng dụng trong lĩnh vực quốc phòng, an ninh.

Đóng góp mới của quá trình nghiên cứu thể hiện trong luận án như sau:

(1) Đề xuất một kiến trúc lồng ghép mới cho m-dãy lồng ghép (một phương pháp mới sinh dãy lồng ghép và lồng ghép phi tuyến) và xây dựng giải pháp bảo mật dữ liệu thoại sử dụng thuật toán sinh số giả ngẫu nhiên dựa trên dãy phi tuyến lồng ghép kiểu mới;

(2) Đề xuất thuật toán cải tiến tốc độ nén, nâng cao chất lượng mã thoại MELPe;

(3) Đề xuất thực hiện kỹ thuật điều chế và giải điều chế để truyền dữ liệu thoại đã

được mã hóa bảo mật qua các thiết bị đầu cuối và mạng (liên mạng) truyền dẫn và đề xuất giải pháp truyền dữ liệu thoại bảo mật qua kênh thoại GSM, các kênh hữu tuyến và vô tuyến băng hẹp khác.

KHẢ NĂNG ỨNG DỤNG TRONG THỰC TIỄN HOẶC NHỮNG VẤN ĐỀ CÒN BỎ NGỎ CẦN TIẾP TỤC NGHIÊN CỨU:

Với những đóng góp khoa học nêu trên, luận án là cơ sở để nghiên cứu, phát triển cho các hệ thống truyền dẫn bảo mật tín hiệu thoại qua kênh thoại GSM và qua các nền tảng khác nhau dựa trên kênh thoại. Các thuật toán, giải pháp và thiết bị được chứng minh và mô phỏng, đánh giá rõ ràng, thực hiện cài đặt thuật toán trên chip FPGA hoặc ARM tạo ra Module được kiểm tra an toàn, thẩm định tính thực thi đúng đắn với lý thuyết để có thể ứng dụng đáp ứng nhu cầu cấp thiết trong thực tế (cụ thể: tùy biến rút gọn để đưa được các chương trình thực thi nén, điều chế biến đổi tín hiệu số chạy trên Vi xử lý STM32).

Liên quan đến những đề xuất mới của luận án, có thể liệt kê những vấn đề cần nghiên cứu trong các công trình tiếp theo như sau:

Phát triển thuật toán nâng cao chất lượng tiếng nói cho phép thiết kế, chế tạo phần cứng thiết bị điện thoại di động, cài đặt các thư viện, các chương trình điều khiển, các thuật toán và hoàn thiện thành một thiết bị điện thoại di động có bảo mật dùng kênh 2G của mạng viễn thông di động GSM đảm bảo tính an toàn trong cài đặt thuật toán vào thiết bị.

Nghiên cứu lý thuyết lấy mẫu theo Nyquist đa băng con để tăng tốc độ điều chế / giải điều chế Modem OFDM, thực thi tích hợp toàn bộ Modem này vào Chip ARM để có thể lắp vào điện thoại di động. Lập trình trên chip với không gian chật hẹp, tài nguyên hạn chế nên yêu cầu phải tối ưu hóa về tốc độ, về kích thước mã chương trình, về không gian vùng nhớ dữ liệu và vùng nhớ phục vụ thao tác tính toán.

Hướng khác là nghiên cứu tích hợp chức năng modem vào phần mềm của điện thoại di động thông minh.

Xác nhận của đại diện tập thể	**Nghiên cứu sinh**
Người hướng dẫn khoa học	
GS. TSKH. Nguyễn Xuân Quỳnh	**Nguyễn Thanh Bình**